Fort Collins, Colorado 80527-2400

ATTORNEY DOCKET NO. 10045121-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Mark CROSBIE	**Confirmation No.:**	2127
Application No.:	09/878,319	**Examiner:**	P. Parthasarathy
Filing Date:	June 12, 2001	**Group Art Unit:**	2136
Title:	SYSTEM AND METHOD FOR HOST AND NETWORK BASED INTRUSION DETECTION AND RESPONSE		

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Sir:

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on July 20, 2005.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

( ) (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d) for the total number of months checked below:

( )	one month	$120.00
( )	two months	$450.00
( )	three months	$1020.00
( )	four months	$1590.00

( ) The extension fee has already been filled in this application.

(X) (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account **08-2025** the sum of **$500.00**. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

( ) I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450. Date of Deposit:_____

OR

(X) I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number 571-273-8300 on 09/20/2005

Number of pages: 19

Typed Name: Randy A. Noranbrock, Y2940

Respectfully submitted,

Mark CROSBIE

By Randy A. Noranbrock

Randy A. Noranbrock

Attorney/Agent for Applicant(s)
Reg. No. **42,940**

Date: 09/20/2005

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of	
Inventor(s): CROSBIE, MARK	: Confirmation No. 2127
	:
U.S. Patent Application No. 09/878,319	: Group Art Unit: 2136
	:
Filed: June 12, 2001	: Examiner: PRAMILA PARTHASARATHY
	:
For: SYSTEM AND METHOD FOR HOST AND NETWORK BASED INTRUSION DETECTION AND RESPONSE	

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Attn: BOARD OF PATENT APPEALS AND INTERFERENCES

BRIEF ON APPEAL

Further to the Notice of Appeal filed July 20, 2005, in connection with the above-identified application on appeal, herewith is Appellant's Brief on Appeal. The Commissioner is authorized to charge Deposit Account No. 08-2025 in the amount of $500 for the statutory fee.

To the extent necessary, Appellant hereby requests any required extension of time under 37 C.F.R. §1.136 and hereby authorizes the Commissioner to charge any required fees not otherwise provided for to Deposit Account No. 08-2025.

09/22/2005 MBINAS 00000009 082025 09878319
01 FC:1402 500.00 DA

TABLE OF CONTENTS

I. Real Party in Interest 3

II. Related Appeals and Interferences 3

III. Status of Claims 3

IV. Status of Amendments 3

V. Summary of Claimed Subject Matter 3

VI. Grounds of Rejection to be Reviewed on Appeal 5

A. Moran Does Not Anticipate Claims 1-8, 10, 12-32, and 35-43 5

B. Moran Does Not Anticipate Claim 9 5

C. Moran Does Not Anticipate Claims 29-32 and 35-43 5

VII. Argument 6

A. Moran Does Not Anticipate Claims 1-8, 10, 12-32, and 35-43 6

B. Moran Does Not Anticipate Claim 9 9

C. Moran Does Not Anticipate Claims 29-32 and 35-43 .. 10

Conclusion 11

Claims Appendix 1

I. REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company L.P.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals and/or interferences.

III. STATUS OF CLAIMS

Claims 1-10, 12-32, and 35-43 are rejected under 35 USC 102(e) as being anticipated by Moran (U.S. Patent 6,647,400). Claims 11 and 33-34 are cancelled.

IV. STATUS OF AMENDMENTS

The Advisory Action mailed July 6, 2005 indicates that the proposed amendments filed June 13, 2005 will not be entered; however, the text of the Action explicitly states, "The substitute specification filed on June 13, 2005 has been entered." As no claim amendments were filed in conjunction with the previous response of June 13, 2005 and based on the explicit statement regarding entry of the substitute specification, Appellant believes that all amendments filed June 13, 2005 are entered and there are no outstanding unentered amendments.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed subject matter of claim 1 concerns a method of detecting intrusions using a host-based intrusion detection system (IDS) 50. (Instant specification at page 11, lines 10-14). IDS 50 examines information about system activity from a variety of data sources including kernel records, i.e., kernel audit data 70. (Instant specification

at page 17, lines 23-25). Kernel records are read and reformatted into a different format, i.e., a memory mapped (mmap) file. (Instant specification at page 22, lines 5-9 and page 24, line 20-page 25, line 2). Advantageously, the mmap file does not require a system call to read or write data from/to the file and thereby provides a low overhead, high bandwidth connection between accessing components of IDS 50. (Instant specification at page 32, lines 14-19). IDS 50 components access the mmap file via a pointer in an address region. Host-based IDS 50 includes a set of pre-configured "patterns" or detection templates 65. (Instant specification at page 28, lines 20-27). The records in the memory mapped file are parsed and compared against one or more templates to detect intrusions. (Instant specification at page 30, lines 19-24 and steps 340, 345, and 350 of FIG. 3).

The claimed subject matter of claim 29 concerns a method of detecting changes to critical files/directories. (Instant specification at page 11, lines 15-20 and page 35, lines 7-page 38, line 5). A predetermined set of files is monitored for modifications, as well as a predetermined set of directories. (Instant specification at page 35, lines 8-12). An alert is generated for each occurrence of a modification of a monitored file. (Instant specification at page 36, line 1 and page 63, lines 16-23). If a directory is specifically excluded and a file in that directory is specifically included then the file is monitored. (Instant specification at page 36, lines 4-6). The predetermined set of files includes a system kernel file and system kernel configuration files. (Instant specification at page 36, lines 24-29). An alert is also generated for each occurrence of a modification of a monitored directory. (Instant specification at page 36, line 3).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

A. Moran Does Not Anticipate Claims 1-8, 10, 12-32, and 35-43

B. Moran Does Not Anticipate Claim 9

C. Moran Does Not Anticipate Claims 29-32 and 35-43

VII. ARGUMENT

A. Moran Does Not Anticipate Claims 1-8, 10, 12-32, and 35-43

The rejection of claims 1-8, 10, 12-32, and 35-43 as being anticipated by Moran et al., U.S. Patent 6,647,400, was incorrect as a rejection based on 35 U.S.C. §102 requires every element of the claim to be included in the reference, either directly or inherently, and Moran fails to include all elements of claim 1. There are at least 3 reasons why Moran fails to anticipated the present claimed subject matter: (1) Moran fails to reformat kernel records into a different format, (2) Moran fails to identify a different format for records is a memory mapped file, and (3) Moran fails to parse the records and compare the records against a template.

Moran discloses a system and method for detecting intrusions in a host system on a network. In operation, Moran includes a configuration discovery mechanism which locates host system files and communicates the locations of the files to an analysis engine. A file processing mechanism matches contents of a deleted file to a directory or filename. A signature checking mechanism computes the signature of a file and compares it to previously computed signatures. (Moran at Abstract).

First, the Examiner's assertion that Moran discloses "reformatting the kernel records in a different format (e.g. dump formats)" is incorrect. (Final Official Action mailed April 20, 2005 at page 4, section 8.) In contrast, Moran at column 11, lines 15-54, discloses, at most, that the system is able to read "dump format" files, but fails to disclose reformatting read kernel records into a different format. See specifically, column 11, lines 33-34, "Filesystem information ... may be recovered from backup dumps."

(emphasis added) In the absence of disclosure in Moran of reformatting read kernel records into a different format, the rejection should be reversed.

Second, even assuming *arguendo* that Moran reformats read kernel records into a different format, Moran fails to disclose that the different format is a memory mapped file. Moran at column 27, lines 37-39, discloses that a directory in a file system is a file which maps a file name to an i-node; however, a directory is not a reformatted kernel record. Additionally, Moran at column 29, lines 4-52, discloses a procedure for finding names of deleted files and not a memory mapped file for reformatted kernel records. Neither of the identified disclosures of Moran disclose a format for reformatted kernel records is a memory mapped file. In accordance with the present subject matter, the memory mapped file is used as an interprocess communication mechanism for sending data between components of the IDS in order to impose a lower overhead on the overall system. (Instant specification at page 16, lines 4-6). Moran fails to disclose either the limitation or the feature as described. For at least this reason, the rejection should be reversed.

Third, contrary to the Examiner's assertion, Moran fails to disclose parsing and comparing records against a template. (Final Office Action at page 4, section 8). Moran at column 18, lines 6-58, and at column 32, lines 44-58, fails to disclose parsing the records and comparing the parsed records against a template. Instead, column 18, lines 6-58 of Moran describes the format for message transfers between sensors of the system and the analysis engine. According to Moran, sensor data may be transferred to the analysis engine using the described message header; however, there is no disclosure

of parsing records and comparing parsed records against a template.

Further, column 32, lines 44-58, of Moran discloses cross checking files with signatures of current versions of the file in a database. Moran fails to disclose comparing records against a template according to the description of a template comparison at page 28, lines 20-27 of the instant specification. Further still, a file signature is not the same as a template. That is, a file signature cannot be used as a representation of an algorithm to detect a vulnerability exploitation. See e.g., instant specification at page 28, lines 21-24, "[a] detection template is a representation of an algorithm to detect a vulnerability exploitation. ... The template contains logic which will process the kernel event stream." For either of these reasons, the rejection should be reversed.

For each of the above reasons, claim 1 is patentable over Moran and the rejection should be reversed.

Claims 2-8, 10 and 12-28 depend, either directly or indirectly, from claim 1, include further important limitations, and are patentable over Moran for at least the reasons advanced above with respect to claim 1 and the rejection should be reversed.

B. Moran Does Not Anticipate Claim 9

The reasons advanced above with respect to claim 1, and incorporated herein, are equally applicable to claim 9 which depends from claim 1. By virtue of at least its dependency on claim 1, claim 9 is patentable over Moran.

Additionally, the rejection of claim 9 as being anticipated by Moran was incorrect as a rejection based on 35 U.S.C. §102 requires every element of the claim to be included in the reference, either directly or inherently, and Moran fails to include all elements of claim 9. The Examiner has repeatedly failed to address Appellant's remarks regarding claim 9 in view of Moran. That is, Moran fails to disclose the claim 9 limitation of encrypting information sent between the intrusion detection system and a network. As stated in the instant specification at page 4, lines 5-6, "[e]ncryption is a mathematical technique that prevents the unauthorized reading and modification of data."

Moran at column 16, lines 15-29, describes the passing of values between components of the system by performing data type conversions and not preventing the unauthorized reading and modification of data. Thus, Moran fails to disclose encrypting information transmitted. Additionally, Moran demonstrates a lack of concern for protecting transmissions as at column 10, lines 17-19, Moran "send[s] the extracted information to another (hopefully uncompromised) computer for analysis." Moran fails to disclose encrypting information sent between the detection system and a network.

For at least this reason and the reasons advanced above with respect to claim 1 from which claim 9 depends, the rejection of claim 9 should be reversed.

C. Moran Does Not Anticipate Claims 29-32 and 35-43

The rejection of claims 29-32 and 35-43 as being anticipated by Moran was incorrect as a rejection based on 35 U.S.C. §102 requires every element of the claim to be included in the reference, either directly or inherently, and Moran fails to disclose that if a directory is specifically excluded and a file in the specifically excluded directory is specifically included the file is monitored. At most, Moran at column 32, line 44-column 33, line 62, describes that "[f]iles in system directories that are not in a package management database or an internal database are flagged as mildly suspicious." The statement relates to how the Moran system handles files which are not in a location at which they are expected to be based on database information regarding the files. There is no disclosure of monitoring a file located in a specifically excluded directory. Moran fails to disclose a specifically included file in a specifically excluded directory and thus cannot disclose monitoring the specifically included file. For at least this reason, the rejection of claim 29 should be reversed.

Claims 30-32 and 35-43 depend, either directly or indirectly, from claim 29, include further important limitations, and are patentable over Moran for at least the reasons advanced above with respect to claim 29 and the rejection should be reversed.

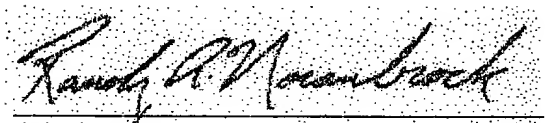
CONCLUSION

For the extensive reasons advanced above, the present claimed subject matter of claims are patentable over and the rejection of claims 1-10, 12-32, and 35-43 should be reversed.

Reversal of the rejection is in order.

Respectfully submitted,

CROSBIE, MARK

By: 

Randy A. Noranbrock
Reg. No. 42,940

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400
Telephone: 703-684-1111
Facsimile: 970-898-0640

KMB:RAN/iyr

CLAIMS APPENDIX

1. A method of detecting intrusions using a host-based intrusion system, comprising:

reading kernel records;

reformatting each of the read kernel records into a different format, wherein the different format is a memory mapped file; and

parsing the records and comparing the parsed records against one or more templates.

2. The method of claim 1, wherein the kernel records include kernel audit logs.

3. The method of claim 2, wherein the kernel audit logs includes information about each system call.

4. The method of claim 1, comprising monitoring system log files.

5. The method of claim 1, comprising a system call.

6. The method of claim 1, wherein the system call was initiated by a library call.

7. The method of claim 3, comprising storing each system call in a circular buffer.

8. The method of claim 1, comprising determining that an intrusion has occurred and generating an alert message.

9. The method of claim 1, comprising encrypting information sent between the host-based intrusion system and a network.

10. The method of claim 1, comprising displaying an alert message that an intrusion has occurred.

12. The method of claim 4, comprising converting the system log files into an ASCII format for comparison against the one or more templates.

13. The method of claim 2, comprising converting the kernel records into an ASCII format for comparison against the one or more templates.

14. The method of claim 1, wherein the one or more templates is a modification of files/directories template.

15. The method of claim 1, wherein the one or more templates is a change to log files template.

16. The method of claim 1, wherein the one or more templates is a SetUID files template.

17. The method of claim 1, wherein the one or more templates is a creation of world-writables template.

18. The method of claim 1, wherein the one or more templates is a repeated failed logins template.

19. The method of claim 1, wherein the one or more templates is a repeated failed SU commands template.

20. The method of claim 1, wherein the one or more templates is a race conditions attack template.

21. The method of claim 1, wherein the one or more templates is a buffer overflow attacks template.

22. The method of claim 1, wherein the one or more templates is a modification of another user's file template.

23. The method of claim 1, wherein the one or more templates is a monitor for the start of interactive sessions template.

24. The method of claim 1, wherein the one or more templates is a monitor logins/logouts template.

25. The method of claim 1, wherein the one or more templates is chosen from the group including:

a modification of files/directories template;

a change to log files template;

a SetUID files template;

a creation of world-writables template;

a repeated failed logins template;

a repeated failed SU commands template;

a race conditions attack template;

a buffer overflow attacks template;

a modification of another user's file template;

a monitor for the start of interactive sessions template; and

a monitor logins/logouts template.

26. The method of claim 1, wherein the kernel records are read from different computers.

27. The method of claim 1, wherein parsed records are compared against the one or more templates using at least one correlator.

28. The method of claim 1, wherein said parsing step compares the parsed records against the one or more templates simultaneously.

29. A method of detecting changes to critical files/directories, comprising:

monitoring a predetermined set of files for modifications;

monitoring a predetermined set of directories for modifications;

generating an alert for each occurrence of a modification of a monitored file , wherein if a directory is specifically excluded and a file in the specifically excluded directory is specifically included then the file is monitored, and wherein the predetermined set of files includes a system kernel file and system kernel configuration files; and

generating an alert for each occurrence of a modification of a monitored directory.

30. The method of claim 29, comprising:

determining which files to monitor of all files on a computer to form the predetermined set of files;

determining which directories to monitor of all directories on a computer to form the predetermined set of directories.

31. The method of claim 29, comprising, for each said determining step, specifically including a file or directory, specifically excluding a file or directory, or not specifically including or excluding a file or directory.

32. The method of claim 29, wherein a file or directory which is not specifically included or excluded is monitored.

35. The method of claim 29, wherein the predetermined set of files includes /stand/vmunix, /stand/kernel and /stand/bootconf.

36. The method of claim 29, wherein the predetermined set of files includes files defining the users on a system and files used to create accounts.

37. The method of claim 29, wherein the predetermined set of files includes /etc/passwd and /etc/group.

38. The method of claim 29, wherein the predetermined set of files includes files which control what network services are running and which controls programs used to fulfill service requests.

39. The method of claim 29, wherein the predetermined set of files includes /etc/inetd.conf.

40. The method of claim 29, wherein the predetermined set of files includes files which are used to control the remote access of the user root without requiring a password.

41. The method of claim 29, wherein the predetermined set of files includes/.rhosts and /.shosts.

42. The method of claim 29, wherein the set of files specifically excluded includes temporary files created by a program view.

43. The method of claim 29, wherein the predetermined set of directories includes /bin, /sbin and /usr/bin.